National Infrastructure Protection Center CyberNotes

Issue #2000-05 *March 15, 2000*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, hacker exploit scripts, hacker trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between February 25 and March 9, 2000. The table provides the hardware/operating system, equipment/software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates from previous issues of CyberNotes are listed in bold. New information contained in the update will appear as red and/or italic text.**

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Alex Heiphetz Group, Inc.[1]	EZShopper 3.0	A vulnerability exists which allows anyone to execute any commands on the remote system with the privileges of the web server. An unauthorized individual can also read any file on the remote system which the webserver has access to.	Download and install the newest version from AHG's website, http://www.ahg.com.	EZShopper Remote Command Execution	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.

[1] Bugtraq, February 27, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Allaire[2]	ColdFusion Server 4.0, 4.0.1, 4.5	A vulnerability exists in the APPLICATION.CFM or ONREQUESTEND.CFM file, which allows a malicious user to obtain the full physical path to that file.	Allaire is aware of the issue and it is fixed as of the 4.5.1 release.	Allaire ColdFusion Path Disclosure	Low	Bug discussed in newsgroups and websites. Exploit has been published.
AOL[3]	Instant Messenger 3.5	A Denial of Service vulnerability exists in AIM (AOL Instant Messenger). This occurs when a message is received that contains an invalid encoded ASCII value.	No workaround or patch available at time of publishing.	AIM Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Axis Communi-cations[4]	StorPoint CD	A vulnerability exists in the authentication required for administration, which could allow malicious users to access administrator URLs without entering username and password.	Upgrade to Software Version 4.28 located at: http://www.se.axis.com/techsup/cdsrv/storpoint_cd/index.html	Axis StorPoint CD Authentication	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
BisonWare[5] ***Patch available soon[6]***	**BisonWare FTP Server 3.5**	**A local/remote Denial of Service vulnerability exists in BisonWare FTP Server when a long user name, 2000 characters is entered.**	**No workaround or patch available at time of publishing.** ***This problem is fixed in V4.1 out soon.***	**Denial of Service Vulnerability**	**Low**	**Bug discussed in newsgroups and websites.** **Exploit has been published.**
Caldera[7]	OpenLinux 2.3	A vulnerability exists in the default installation of Caldera OpenLinux 2.3. which allows a malicious user to obtain a listing of the packages, and versions of packages installed on the system. This could be used to determine potential vulnerabilities on the machine remotely.	Temporary workaround: Remove or disable this program. # chmod 0 /home/httpd/cgi-bin/rpm_query	Caldera OpenLinux 2.3 rpm_query CGI Vulnerability	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Corel[8]	Linux OS 1.0	Local users can take advantage of a packaging and configuration error to execute arbitrary commands as root.	Patch available at: http://www.dosemu.org/docs/README/0.98/README-3.html	Corel Linux Dosemu Distribution Configuration	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.

[2] Bugtraq, March 5, 2000.
[3] Securiteam, March 7, 2000.
[4] Infosec Security Vulnerability Report, February 29, 2000.
[5] UssrLabs, November 24, 1999.
[6] Labs Advisory Code: RLA002, February 29, 2000.
[7] Bugtraq, March 4, 2000.
[8] Bugtraq, March 3, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Corel[9]	Corel Linux artCorel xconf	Local malicious users can take advantage of the lack of input validation and privilege dropping to gain root access.	No workaround or patch available at time of publishing.	ArtCorel xconf Validation	**High**	Bug discussed in newsgroups and websites. Exploit script has been published
Debian, RedHat[10, 11]	NMH 1.0.2 and prior (distributed with Debian GNU/Linux 2.1, Red Hat Linux 5.2, 6.0, 6.1)	A buffer overflow vulnerability exists in the nmh mailer, which could allow a malicious user to execute arbitrary code and potentially lead to remote access.	Upgrading to the latest version of nmh is recommended by the program authors which is available at: ftp://ftp.mhost.com/pub/nmh/nmh-1.0.3.tar.gz	nmh Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Deerfield[12]	Cat Soft Serv-U 2.5d	The default settings for Serv-U cause the server to give out full physical path information, which could be used to simplify other potential attacks.	There is an option to change the messages to a less informative format. This has to be done for each user or group.	Serv-U FTP Server Path Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
DNSTools Software[13]	DNSTools 1.0.8	A vulnerability exists in the 1.0.8 release of DNSTools (labeled on some areas of their site as 1.08). By manipulating the contents of certain post variables, arbitrary code may be executed.	No workaround or patch available at time of publishing.	DNSTools Input Validation	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
FreeBSD[14]	MySQL	A vulnerability exists in the password authentication mechanism in MySQL database server which would let a malicious user bypass the authentication mechanism	Upgrade or reinstall a new package obtained from: ftp://ftp.FreeBSD.org/ports/	MySQL Password Authentication	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Foundry Networks[15]	ServerIron 5.1.10t12, 6.0	A sequence predictable TCP implementation vulnerability exists which could lead to a variety of session hijacking, and blind session spoofing attacks. This can result in the manipulation of these switches.	Foundry has issued a response to the vulnerabilities described. That document is available at: http://www.foundrynet.com/bugTraq.html They have also indicated that firmware upgrades will be available shortly.	ServerIron TCP/IP Sequence Predictability Vulnerability	**High**	Bug discussed in newsgroups and websites.

[9] Securiteam, February 26, 2000.
[10] Debian Security Advisory, 00-005, March 1, 2000.
[11] RHSA-2000:006-01, March 6, 2000.
[12] SecurityFocus, February 20, 2000.
[13] Securiteam, March 6, 2000.
[14] FreeBSD Security Advisory, SA-00:05, February 28, 2000.
[15] Bugtraq, February 28, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Hewlett-Packard[16]	OpenView OmniBack II 2.55, 3.0, 3.1	Multiple open connections to port 5555 can cause the HP OpenView OmniBack program to crash by consuming 100% CPU cycles.	No workaround or patch available at time of publishing.	HP OpenView OmniBack Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Internet Security Systems[17]	RealSecure 3.0, 3.1, 3.2, 3.2.1999	Under certain versions of Internet Security Systems RealSecure Network Intrusion Detection Software (NIDS) it is possible to launch CGI attacks against webservers without the NIDS detecting the attacks properly. Also it is possible for malicious users to launch a series of IP fragment based Denial of Service attacks without the software detecting them properly.	No workaround or patch available at time of publishing.	RealSecure CGI and Denial of Service Attack Subversion	Low	Bug discussed in newsgroups and websites. Exploit has been published.
iPlanet[18]	Web Server Enterprise Edition 4.1	A vulnerability exists that consumes all available memory when a few hundred "Get" requests are sent.	No workaround or patch available at time of publishing.	iPlanet Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
MandrakeSoft RedHat[19]	MandrakeSoft Linux Mandrake 7.0; RedHat Linux 6.1, 6.2	Printtool is an X11 printer configuration tool shipped with RedHat Linux and possibly other Linux distributions. When configuring a printer with printtool, the permissions of the config file are set world-readable. It is possible to obtain the printer share password since it is stored in this world-readable file	No workaround or patch available at time of publishing.	Printtool Config File Permissions	**Medium**	Bug discussed in newsgroups and websites. Exploit has been published.

MandrakeSoft RedHat SuSE[20]	RedHat Linux 5.1, 5.2, 6.0, 6.1, 6.2;
	Linux Mandrake 6.1, 7.0;
	SuSE 6.2
		RedHat Linux (and possibly other distributions) ship with a file backup utility called 'dump'. A vulnerability exists in this application which could allow arbitrary code to be executed and lead to a complete system compromise.	No workaround or patch available at time of publishing.	Linux "dump" Buffer Overflow	**High**	Bug discussed in newsgroups and websites.

[16] Bugtraq, February 28, 2000.
[17] Bugtraq, February 29, 2000.
[18] Securiteam, February 26, 2000.
[19] Bugtraq, March 9, 2000.
[20] Bugtraq, February 28, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft[21]	Wordpad	A security vulnerability exists which enables embedding arbitrary commands in a Wordpad document. These commands are executed, without warning the user, when activating an embedded or linked object.	Workaround: Do not activate objects in the Wordpad document, or use Word to open such files.	Wordpad Embedded Command	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[22]	Clip Art 1.0	A vulnerability exists within the Microsoft Clip Art Gallery, where a remote malicious user can crash the Clip Art application and/or possibly execute arbitrary code.	Microsoft has released a fully supported patch located at: http://cgl.microsoft.com/clipgallerylive/pss/bufovrun.htm	Microsoft Clip Art Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[23]	Internet Explorer 5.0 for Windows 95/98/2000/ NT, 5.01	Security vulnerability in Internet Explorer allows malicious web administrators to insert files with the extension of .chm, which are used by Windows help, and may cause it to execute arbitrary code, possibly compromising the host's security.	Temporary workaround: Disable Active Scripting	Microsoft Internet Explorer HTML Help Shortcut Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Microsoft[24]	Windows 2000	A Denial of Service vulnerability exists in the disk quota feature.	No workaround or patch available at time of publishing.	Windows 2000 Disk Quota Limitation	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[25]	Outlook 97/98/2000; Windows Messaging, Exchange Client	A security vulnerability in Windows Messaging components exist that could allow a malicious user to create a Denial of Service mailbomb attack.	No workaround or patch available at time of publishing.	Microsoft Mail Clients Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Microsoft[26]	Windows NT 4.0	A vulnerability exists in the shared startup folder, which could allow a malicious user to specify a folder with a shortcut to a program of their choice that will be run any time a user logs in, at the privilege level of that user.	Microsoft has released a hotfix that tightens permissions on this and other keys in the registry. The fix is available at: Intel: http://www.microsoft.com/downloads/release.asp?ReleaseID=19172 Alpha: http://www.microsoft.com/downloads/release.asp?ReleaseID=19173	Microsoft Registry Permissions	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[21] Bugtraq. February 25, 2000.
[22] Microsoft Security Bulletin, (MS00-015), March 7, 2000.
[23] Securiteam, March 3, 2000.
[24] Securiteam, March 3, 2000.
[25] Weekly Microsoft Security Roundup, March 2-3, 2000.
[26] Microsoft Security Bulletin (MS00-008), March 9, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft[27]	SQL Server Version 7.0; Data Engine (MSDE) 1.0.	A vulnerability exists which could allow the author of a malicious SQL query to take unauthorized remote actions on a SQL Server or MSDE database or on the underlying system that was hosting the SQL Server or MSDE database.	Patch available at: http://www.microsoft.com/downloads/release.asp?ReleaseID=19132	SQL Query Abuse	**High**	Bug discussed in newsgroups and websites.
Microsoft[28]	Windows 95/98	A Denial of Service vulnerability exists when a local/remote malicious user uses a specially crafted path string that refers to a device driver (rather than a normal URL).	No workaround or patch available at time of publishing.	Windows 95/98 Device Driver Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published
Multiple Vendors[29, 30]	Turbo Linux 3.5b2, 4.2, 4.4, 6.02; Matt Kimball and Roger Wolff mtr 0.28, 0.41	A potential vulnerability exists in the 'mtr' program, by Matt Kimball and Roger Wolff. Versions prior to 0.42 incorrectly dropped privileges on all Unix variants except HPUX, which could lead to obtaining root privileges.	Users of mtr should upgrade to version mtr-0.42 or later. TurboLinux has issued a new package to fix this problem in versions 6.0.2 and prior.	Multiple Vendor mtr	**High**	Bug discussed in newsgroups and websites.
Netscape[31]	Netscape Enterprise Server 3.6SP2	A GET request containing over 4080 characters will cause the httpd.exe process to crash within Netscape Enterprise Server 3.6, resulting in a Dr. Watson error. Arbitrary code can be executed remotely at this point.	No workaround or patch available at time of publishing.	Netscape Enterprise Server GET Request	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Nortel Networks[32]	Netgear ISDN 348.0RH, 328.0RT	NetGear's ISDN router contains a few vulnerabilities that allow remote malicious users to perform a Denial of Service attack against them.	No workaround or patch available at time of publishing.	Nortel Netgear ISDN RH348 and RT328 Denial Of Service	Low	Bug discussed in newsgroups and websites.

[27] Microsoft Security Bulletin, (MS00-014), March 8, 2000.
[28] SecurityFocus, March 4, 2000.
[29] TurboLinux Security Announcement, TLSA2000003-1, March 8, 2000.
[30] Bugtraq, March 3, 2000.
[31] S.A.F.E.R. Security Bulletin, 000229.EXP.1.3, February 29, 2000.
[32] Bugtraq, February 25, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Oracle[33]	Oracle8i 8.1.5	A vulnerability exists in the installation program, which could allow a malicious user the ability to compromise the root account.	No workaround or patch available at time of publishing.	Oracle for Linux Installer	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
RedHat[34]	Linux 4.0-4.2, 5.0-5.2, 6.0-6.2; TurboLinux 6.0.2 and earlier	A buffer overflow exists in the implementation of the 'man' program, which could allow a malicious user to gain egid man.	No workaround or patch available at time of publishing.	RedHat Man Buffer Overrun	**High**	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Rit Research Labs[35]	The Bat! 1.39	Two security vulnerabilities exist which could assist a remote malicious user in compromising the operating system.	No workaround or patch available at time of publishing.	The Bat! X-BAT-FILES Vulnerabilities	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Sambar[36]	Sambar systems prior to 4.2 beta 8	A security vulnerability exists if the default CGIs are left in the CGI-BIN directory, which allows sensitive information to be gained about the remote host.	No workaround or patch available at time of publishing.	Sambar Sensitive Information	Medium	Bug discussed in newsgroups and websites.
SGI[37]	IRIX 6.5	A security vulnerability exists in the infosrch.cgi, which enables remote malicious users to execute arbitrary commands.	No workaround or patch available at time of publishing.	SGI InfoSearch fname	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
SGI[38]	IRIX 5.x, 6.x	A vulnerability exists in the fam daemon, which could allow a malicious user to learn the names of files and directories on IRIX systems.	A version of fam that fixes this vulnerability is available as open source.	AGI Fam Unauthorized Access	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Sun Microsystems[39]	StarScheduler/ StarOffice 5.1	A buffer overflow exists in the StarScheduler web server (which listens on port 801), that can lead to remote execution of code and root access. Another vulnerability exists in the server that allows any user to gain read access to files to which they normally don't have access to.	No workaround or patch available at time of publishing.	StarScheduler/ StarOffice Denial of Service and Arbitrary File Read Vulnerabilities	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[33] Bugtraq, March 5, 2000.
[34] Bugtraq, February 26, 2000.
[35] Securiteam, March 7, 2000.
[36] Bugtraq, February 25, 2000.
[37] SecurityFocus, March 3, 2000.
[38] Network Associates, Inc. Advisory NAI-0016, March 7, 2000.
[39] S.A.F.E.R. Security Bulletin, 000309.EXP.1.4, March 9, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
The Ht://Dig Group[40]	Ht://Dig prior to 3.1.5 (multiple vendors)	There is a security hole in the htsearch cgi-bin program, which allows remote malicious users to read any file on the local system that is accessible to the user ID running htsearch (usually the user ID running the webserver process, user 'nobody' in the default installation of apache).	ht://dig version 3.1.5 is fixed, and is available at: http://www.htdig.org/files/htdig-3.1.5.tar.gz The fixed beta version, 3.2.0b2, should be available shortly. For more information check ht://dig's webpage at: http://www.htdig.org/ TurboLinux: ftp://ftp.turbolinux.com/pub/updates/6.0/security/htdig-3.1.5-1.i386.rpm	ht://dig Arbitrary File Inclusion	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Trend Micro[41]	OfficeScan 3.5	Numerous security vulnerabilities exist which could allow malicious users to start a scan, stop a scan, modify the scan configuration and write arbitrary files on the target machine.	No workaround or patch available at time of publishing.	Trend Micro OfficeScan Denial of Service	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
University of Kansas[42]	Lynx 2.7, 2.8, 2.8.3dev2x	Several buffer overflow conditions exist in versions of Lynx that could allow a remote user to gain access to the machine Lynx is being run from.	No workaround or patch available at time of publishing.	Lynx Long URL Buffer Overflow	**High**	Bug discussed in newsgroups and websites.

*Risk is defined in the following manner:

High - A vulnerability that will allow an intruder to immediately gain privileged access (e.g., sysadmin, and root) to the system. An example of this would be a vulnerability in which a sequence of instructions is sent to a machine by an unauthorized user and the machine responds with a command prompt.

Medium - A vulnerability that will allow an intruder immediate access to the system that is not privileged access. This allows the intruder the opportunity to continue the attempt to gain root access. An example would be a configuration error that allows an intruder to capture the password file.

Low - A vulnerability that provides information to an intruder that could lead to further compromise attempts or a Denial-of-Service (DoS) attack. The reader should note that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered as a "High" threat.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between February 25 and March 6, 2000, listed by date of script, script names, script description, and comments.

[40] FreeBSD Security Advisory: FreeBSD-SA-00:06.htdig, March 1, 2000.
[41] Bugtraq, February 25, 2000.
[42] Bugtraq, February 27, 2000.

Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that hackers/crackers are utilizing. During this period, 54 scripts, programs, and net-news messages containing holes or exploits were identified.

Date of Script (Reverse Chronological Order)	**Script Name**	**Script Description**	**Comments**
March 6, 2000	Vncdec.c	Decrypts the password for VNS, a PCAnywhere like program.	
March 6, 2000	Nmap-2.3BETA15.tgz	A utility for network exploration or security auditing. It supports ping scanning, many port scanning techniques, and TCP/IP fingerprinting.	
March 6, 2000	NSS_2000pre8.tar.gz	Narrow Security Scanner 2000 searches for 365 remote vulnerabilities. Written in Perl, and tested on RedHat, FreeBSD, OpenBSD, Slackware, and SuSE.	
March 6, 2000	**Flog.c**	**Script that crashes Windows 95/98/ webservers by sending GET/con/con HTTP/1.0.**	
March 4, 2000	Rlbison.tgz	Denial of Service exploit script for the remote buffer overflow vulnerability in BisonWare FTP Server.	
March 4, 2000	STC3.zip	A multipurpose tool for Windows that does the work of 30 separate programs. Includes a .htaccess Brute-Forcer, Anonymous FTP Scanner, List of Bios Master Passwords, tiny CD-Player g.CGI-Vulnerability Scanner, Country Codes List, Dictionary Generator, DNS Domain Scanner, File Compare, FTP Brute-Force Service Scanner, Cached ISP Passwords Retriever and more.	
March 3, 2000	Binds.c	IRIX 5.3 and 6.2 remote bind iquery overflow.	
March 3, 2000	SXe.c	Sends IGMP packets, denying service to Windows machines.	
March 3, 2000	Etheral-0.8.4.tar.gz	A GTK+ based network protocol analyzer, or sniffer, that lets you capture and interactively browse the contents of network frames.	
March 3, 2000	Ethereal-0.8.4.zip	Ethereal for Windows.	
March 3, 2000	Sps3.c	Spaghetti Proxy Server 3.0 Denial of Service exploit script.	
March 3, 2000	Reap-2.9.tar.gz	Scans any number of IPs for vulnerable CGIs, misc. daemons and a few other remote exploits, while saving banners for future reference.	
March 3, 2000	Ports.c	TCP Portscanner that allows you to choose the range of ports to scan.	
March 2, 2000	Sara-2.1.9.tar.gz	A security analysis tool based on the SATAN model which checks for common old holes, backdoors, trust relationships, default cgi, and common logins.	
March 2, 2000	**Crash-ie.txt**	**Demonstration exploit that crashes Internet Explorer.**	
March 2, 2000	Unsigned.cab.exploit.txt	Vulnerability details and example exploit for Microsoft's Active Setup control's unsigned CAB file execution vulnerability.	
March 2, 2000	**Ie5-chm.txt**	**Demonstration exploit for the Internet Explorer 5.x .chm file vulnerability.**	

Date of Script **(Reverse Chronological Order)**	**Script Name**	**Script Description**	**Comments**
March 2, 2000	Nessus-0.99.7.tgz	Remote security scanner for Linux, BSD, Solaris, and some other systems.	
March 2, 2000	Bsd-sm884.c	FreeBSD Sendmail 8.8.4 mime 7 to 8 remote exploit script.	
March 2, 2000	Mailer.c	Script which exploits the remote Mailer 4.3 vulnerability.	
March 1, 2000	**hp-omniback.pl**	**Demonstration script in Perl, which exploits the HP-OpenView Denial of Service vulnerability.**	
March 1, 2000	**manxpl.c**	**Linux x86 man exploit - exploits the stack overflow in man (PAGER env var) yielding egid man.**	
March 1, 2000	Sara-2.1.8a.tar.gz	Security analysis tool based on the SATAN model which checks for common old holes, backdoors, trust relationships, default cgi, and common logins.	
March 1, 2000	Getpop3.txt	Exploit for the Linux GETpop3 POP vulnerability, which makes any local file world writable.	
March 1, 2000	Dosemu.sh	Script that exploits the Corel Linux dosemu config error vulnerability that could lead to root compromise.	
March 1, 2000	**Setxconf.sh**	**Script that exploits the Corel xconf utils local root vulnerability.**	
March 1, 2000	Saint-2.0.beta1.tar.gz	Security assessment tool based on SATAN whose features include scanning through a firewall, updated security checks from CERT & CIAC bulletins, 4 levels of severity (red, yellow, brown & green) and a feature rich HTML interface.	
March 1, 2000	Infosec.200000229.axisstorpointcd	Technique for exploiting the Axis StorPointCD vulnerability.	
March 1, 2000	**Hp-omniback.pl**	**Demonstration exploit for the HP OpenView OmniBack vulnerability.**	
March 1, 2000	Htdig.txt	Exploit information for the Htdig 3.1.4 vulnerability.	
March 1, 2000	**Manxpl.c**	**Linux x86 man exploit, which exploits the stack overflow in man vulnerability.**	
March 1, 2000	Diemirc.c	MIRC 5.7 Denial of Service exploits.	
February 29, 2000	**agroMANauer.c**	**Script that exploits the man vulnerability.**	
February 29, 2000	Spike.sh5.2.tgz	Denial of Service attack tool, which includes 33 DoS attacks at once, launched from a 61k-shell script.	
February 29, 2000	Mssqlpwd.zip	MS SQL 6.5/7.0 brute force password-cracking tool.	
February 29, 2000	Nessus-0.99.6.tar.gz	Full feature remote security scanner for Linux, BSD, Solaris and some other programs.	
February 28, 2000	Pirchslap.c	Pirch 98 IRC client ident/fserve daemon Denial of Service overflow attack.	
February 28, 2000	**Newsbug.txt**	**Demonstration exploit for Netscape and Outlook Denial of Service vulnerabilities.**	

Date of Script **(Reverse Chronological Order)**	**Script Name**	**Script Description**	**Comments**
February 28, 2000	Toast.0.1.tgz	Shell script that launches 49 different Denial of Service attacks against a victim IP.	
February 28, 2000	Wpack1.2b.zip	Remote administration tool, which is a Windows Trojan coded in Delphi.	
February 28, 2000	Le_guardien.zip	Windows Trojan written in VB6 with many remote control functions.	
February 28, 2000	md-webscan-1.0.1.tar.gz	A high quality CGI vulnerability scanner.	
February 28, 2000	010.txt	EZ Shopper 3.0 remote exploit.	
February 26, 2000	**Redhat_man.c**	**RedHat /usr/bin/man exploit script which could lead to potential root compromise**	
February 25, 2000	Mmsu-dos.c	Denial of Service exploit for the Microsoft Media Server 4.1 vulnerability.	
February 25, 2000	008.txt	Exploit description for the Corel Linux 1.0 dosemu distribution configuration vulnerability.	
February 25, 2000	**Nb16_p04.zip**	**NetBus 6\1.6 (Patch 4) patched to avoid detection by Spider, Drweb. Avp and Norton Antivirus.**	
February 25, 2000	**Bo120p08.zip**	**Back Orifice 1.20 (Patch 8) patched to avoid detection by Drweb, Avp, and Norton Antivirus.**	
February 25, 2000	**Icqtrp02.zip**	**ICQ Trojan patched to avoid detection by Drweb, Avp, and Norton Antivirus.**	
February 25 2000	**Gf_p02.zip**	**Girlfriend remote control Trojan patched to avoid detection by Drweb, Avp and Norton Antivirus.**	
February 25, 2000	NSS-2000pre71.tar.gz	Narrow Security Scanner 2000 searched for 341 remote vulnerabilities.	
February 25, 2000	Aicmpsend.tar.gz	An ICMP packet sender featuring implementation of all ICMP flags and codes, spoofing, and flooding.	
February 25, 2000	Ucgi200.c	CGI vulnerability scanner that checks for 173 CGI vulnerabilities.	
February 25, 2000	HTTP-XpsScanner.tgz	Scans a remote webserver for 77 vulnerable CGI scripts.	

Script Analysis

This section will supply a short description of scripts that have been analyzed by various security professionals and organizations. If you or your organization wish to contribute, please send e-mail to nipc@fbi.gov with the subject line “CyberNotes Script Analysis.” While this section will list only short descriptions, contributors are requested to include a full technical analysis of the script along with release instructions. The release categories are: releasable to anyone; limited releasability (originator-defined list of organizations); or provided for NIPC only. If you would like to receive a copy of the full technical analysis version of any summarized analysis, please send an e-mail listing the script name and requesting the full technical analysis. A member of the CyberNotes editorial team will contact you. All contributions will be credited to the contributing individual or organization unless otherwise requested.

Trends

Trends for this two-week period:

DDOS/DOS:

A Denial of Service attack tool, stream.c, has been discovered which could cause Unix machines to stop responding. It floods the host with ACK's coming from random IPs with remote sequence numbers. This type of attack may be difficult to filter out, as it may resemble "normal" traffic.

There has been an increase in intruders attempting to compromising systems and install Distributed Denial of Service (DDoS) tools, such as Trin00, TFN, TFN2K, Stacheldraht or Troj_Trinoo, for launching packet-flooding Denial of Service attacks. More information regarding these type of attacks may be found at the CERT or NIPC web sites: http://www.cert.org and http://www.nipc.gov respectively. One of the ways organizations can assist in stopping these DDoS attacks is to place egress filters on their gateways. A SANS paper on egress filtering can be found at http://www.sans.org/y2k/egress.htm

A new Windows 9x Denial of Service named twinge.c has been made available. The DoS sends all possible types of ICMP traffic, making Windows 9.x systems crash immediately.

The newly discovered Poison Null and Upload Bombing security attacks could let crackers cripple many interactive websites. Both attacks exploit vulnerabilities in CGI programs that translate between the HTML used in Web pages and the servers that run interactive websites.

Other:

There has been an increase in the recent distribution of worm variants of Melissa and PrettyPark.

An increase in activity related to compromises of Microsoft IIS web servers due to exploitations of a well-known vulnerability in Microsoft Data Access Components (MDAC).

An increase in reports indicating a rise in activity related to a Visual Basic Script (VBScript) known as "network.vbs".

Intruders are actively exploiting Windows networking shares that are made available for remote connections without requiring password authentication.

There has been an increase in systems being compromised via the WU-FTP or WU-FTPD vulnerabilities. There has also been an increase in systems being root compromised via the 'NXT' vulnerability in BIND. Also, numerous systems are being root compromised via the sadmind (port 111 - sunrpc) vulnerabilities.

Increases in SSH attack attempts.

There has been an increase in port scans from Argentina and an increase in scans from Korean hosts that are aimed at port 111, 2974, and 4333. There has also been are reported increase in probes on ports 1080, 1953, and 31337. An increase in probes to ports 109/tcp, 137/udp, 138/udp, and 139/tcp has also been reported.

Viruses

SouthPark (Internet worm): This is a variant of the PrettyPark worm discovered earlier this year. The Trojan Horse has been reported on Windows NT and 9x machines at dozens of large corporations, government organizations, universities and Internet companies, primarily in the U.S. but also in Asia and Europe.

The Trojan Horse spreads by sending itself as an e-mail attachment to all the addresses listed in a user's Outlook Express program. It attempts to do this every 30 minutes, and has the potential to cause e-mail storms that can clog up a company's networks.

The Trojan Horse may also try to connect to an Internet relay chat server, and could potentially use the connection to get information such as the computer name and registered owner, as well as dial up Networking and user names stored on that computer.

Outlook Express users should be aware of e-mails that carry the subject line, "C:/coolprogs/prettypark.exe." File attachments are called "Pretty park.exe" and in some cases "Pretty~1.exe."

WM97/Blaster-A (Word 97 macro virus): This Word macro virus has a similar payload to WM97/Cont. On the 17th of any month this virus changes C:\AUTOEXEC.BAT. The changes attempt to delete all files from the C:, D:, E:, and F: hard drives the next time the computer is rebooted.

WM97/Ethan-BY (Word 97 macro virus): This virus has been reported in the wild. It is a variant of the WM97/Ethan Word macro virus. Whenever an infected document is closed there is a 1 in 3 chance of a File|Properties|Summary box appearing on the screen with the title Ethan Frome.

WM97/Ethan-CC (Word 97 macro virus): This is another variant of the WM97/Ethan Word macro virus, and uses the same infection method but contains none of the other payloads. The virus intercepts when an infected document is closed and saves an infected copy in the directory C:\winbackup.

WM97/Lenni-A (Word 97 macro virus): This is a Word macro virus. If the year is 2000 and an infected document is closed the virus attempts to format the C: drive.

On the 1st January, 10th January, 20th January, 1st April, 4th August, and 31st October in the year 2000 the virus displays a message box titled "-= MILLENNIUM VIRUS =-" containing the text "Alert..!! Your PC have a serious problem with the Year 2000".

WM97/Marker-CQ (Word 97 macro virus): This is a variant of WM97/Marker. On any date after June 2000 this virus will create up to 999999991copies of the infected document in the c:\windows directory. The virus also contains the constant "la macro de colombia xxx".

WM97/Marker-CU (Word 97 macro virus): This is a variant of the WM97/Marker-R Word macro virus. Between September 15th to September 30th the virus displays a message box saying:

"Did you wish the Daredevil on his Birthday?"

The message box has two buttons marked "Yes" and "No". If you click "Yes" another message box appears:

"Thank You! I love you. You are really sexy."

However, if you click "No" a message box appears saying:

"You are Heart Less.
You Will Be Punished"

The virus then attempts to disconnect non-local drives.

The virus contains the following text, which does not get displayed:

"Happy Birthday Daredevil. We'll always remember you."
"The Daredevil's Birthday falls on the 15th of September.
Don't Forget to wish him."

WM97/Melissa-AM (Word 97 macro virus and e-mail worm): WM97/Melissa-AM is another variant of the Melissa Word macro virus. If you have more than 10 addresses in any of your Outlook address books the virus forwards itself via e-mail to between 30-60 percent of the addresses. It randomly sets the importance level of the e-mail to Low, Medium or High. The subject line used by the virus in the e-mail message it forwards is created randomly from phrases to construct a sentence:

"Hello!", "Hi!",

"Here", "I think this", "Gee...Guess this"
"is", "used to be", "are"
"that", "the", "your"
"file", "document", ".doc"
"you requested", "they asked"

In this way subject lines used by the virus when it forwards itself could include:

"Hello! I think this used to be your document you requested"
or
"Hi! Gee...Guess this are the file they asked"

Attached to the e-mail will be an infected Word document. If the recipient opens the document in Microsoft Word the virus will infect them.

WM97/Melissa-AM also sends system information, such as your user name, time zone and registered user details to several fixed e-mail addresses: infx@iname.com, fafx@fastermail.com and apfx@apexmail.com.

WM97/Myna-G (Word 97 macro virus): WM97/Myna-G is a Word macro virus that contains no intentionally malicious code. The replicating code contains the phrase MYNAMEISVIRUS, which is used as a flag to check for its presence.

WM97/Myna-H (Word 97 macro virus): WM97/Myna-H is another Word macro virus that contains no intentionally malicious code. The replicating code contains the phrase MYNAMEISVIRUS, which is used as a flag to check for its presence.

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. The increasing number of Trojans gains added significance due to recent testing conducted to determine the ability of anti-virus software to detect Trojans. According to the test results, a number of popular anti-virus products failed to detect or had limited detection capabilities against current popular Trojans. Testing also indicates that detection of a baseline Trojan does not necessarily mean the anti-virus software can detect a variant. Readers should contact their anti-virus vendors to obtain specific information on Trojans and their variants that their software detects.

The following table provides the reader with a list of Trojans that have received write-ups in this publication. This table starts with Trojans discussed in CyberNotes #2000-01 and will be added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks.

Trojan	Version	Issue discussed
AOL Trojan		CyberNotes-2000-01
DeepThroat	**v1.0 - 3.1 + Mod (Foreplay)**	**Current Issue**
Delta Source	J0.5b-0.7	CyberNotes-2000-01
Donald Dick	1.52-1.55	CyberNotes-2000-01
FakeFTP	Beta	CyberNotes-2000-02
Girlfriend	**V1.3x (including Patch 1 & 2)**	**Current Issue**
Hack'A'tack	1.0-2000	CyberNotes-2000-01
InCommand	1.0-1.4	CyberNotes-2000-01
Intruder		CyberNotes-2000-01
Kuang Original	0.34	CyberNotes-2000-01

Matrix	1.4-2.0	CyberNotes-2000-01
Softwarst		**Current Issue**
SubSeven	1.0-2.1c	CyberNotes-2000-01
SubSeven	1.0-2.1Gold	CyberNotes-2000-02
Trinoo		**Current Issue**
TryIt		**Current Issue**
wCrat	**v1.2b**	**Current Issue**

DeepThroat v1.0 - 3.1 + Mod (Foreplay) (February 27, 2000): This Trojan adds a registry line not only when its run, but when its shutdown. Version 1 used the name System32, and version 2 and 3 uses the name SystemTray. This key will be located in HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

For version 1, look for the item 'System32', which should point to the file c:\windows\system32.exe
Version 2 or 3 will be listed under the item 'Systemtray', and should point to c:\windows\systray.exe
(*Note:* ***If you have an item 'SystemTray' = 'Systray.exe' with no path, then this points to C:\windows\system\ and is OK. Only copies residing in C:\windows are potentially dangerous***.)

There is also a version, actually a modification to the DeepThroat server, called 'Reduced Foreplay'.

Girlfriend v1.3x (Including Patch 1 and 2) (February 28, 2000): Girlfriend is designed to let you steal information from the infected PC. Below is a list of some of its features:

text, that "infected" user enters to any window containing password field;
passwords, which "infected" user enters to password fields.
send "system" messages to remote PC;
play sounds;
show bitmaps (.bmp pictures);
send "victim" to any URL;
change server's port;
hide GF Client with BOSSKEY=F12;
scan subnet for infected servers;
ping server;
save windows list;
also takes passwords from Web sites, which infects user inputs!

Softwarst (February 27, 2000): Softwarst is a Trojan that can upload and download files, run programs, monitor your computer in real time (Keylogger and screen capture) edit registry and even format your harddisk with a single button click.

Troj_Trinoo (February 27, 2000): Trinoo is a Distributed DoS attack Trojan. The idea is that one person, or group of people, control many infected computers at the same time. They can cause each of these infected systems to attack one specified computer at their request.

Most DoS attacks are caused on one computer with an extremely large amount of bandwidth. However many hundreds of computers all with very small amounts of bandwidth (i.e. modem dialups), may be used instead. This appears to be the purpose of this Trojan. A machine infected with this Trojan not only can have his own bandwidth wasted, but is helping contribute to attacks against others.

Trinoo is not a virus, but an attack tool released in late December 1999, used to perform a distributed DoS attack. Trinoo's master component is the component that actually performs the attack. Master component is typically secretly installed on a hacked computer, or Zombie, on the Internet. Trinoo's master component is capable of broadcasting many UDP packets to a designated or targeted computer. The targeted computer tries to process and respond to these invalid UDP packets with "ICMP port unreachable" messages for each UDP packet. Because it has to respond to so many of them, it eventually runs out of network bandwidth, which results in a denial of service. Trinoo also has a client component that is used to control the master component. This lets the hacker control multiple master components remotely. The client can communicate with the master component by sending various commands.

W32.DoS.Trinoo is a Windows compiled version of the Trinoo master component, although Trinoo can also be compiled under UNIX platforms such as Linux. When W32.DoS.Trinoo is executed, it is copied into the windows system directory as service.exe. It modifies the registry to load itself each time the computer is started. Once W32.DoS.Trinoo is in memory, it listens for a command such as mdos, mping, mdie, dos, mtimer, or msize from the Trinoo client program and performs the associated tasks. It is important to detect the Trinoo master component because it can be installed secretly on your computer system by a hacker.

TryIt (February 27, 2000): Tryit comes in two forms, each of which pretends to delete all the files in your C:\windows directory. Your windows directory is indeed safe however. What they secretly do is install a pre-configured rc5 client that causes your computer to help process rc5 data.

wCrat v1.2b (February 29, 2000): The wCrat Trojan can up/download files, run programs, contains a key logging, and changes quite a number of Windows settings.